@chadmcrowell.com
/in/chadmcrowell
kubeskills.com

CYBR

Detecting and Responding to Threats

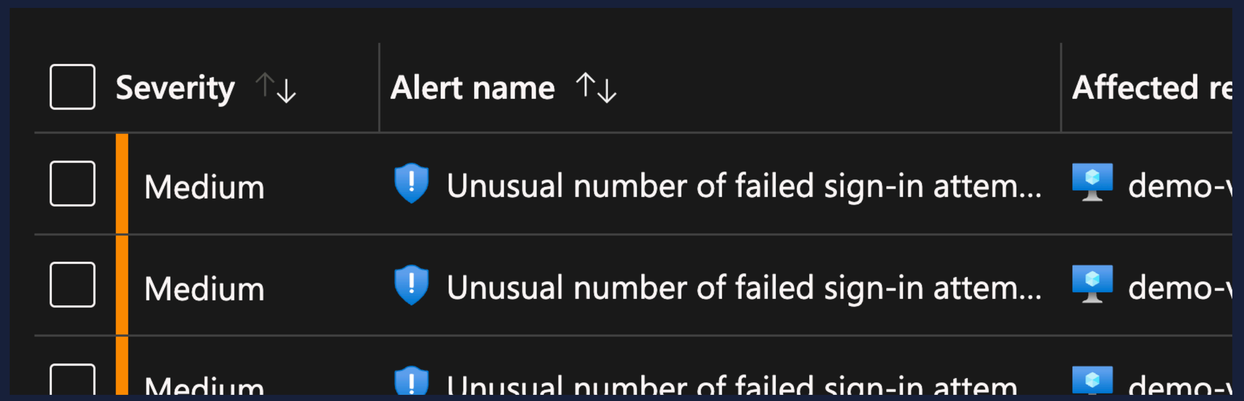
@chadmcrowell.com
/in/chadmcrowell
kubeskills.com

CYBR

Microsoft Defender for Cloud

Detecting & Responding to Threats

- Alerts are generated when suspicious or malicious activity is detected across your Azure or hybrid environment
- Alerts are powered by Microsoft threat intelligence, machine learning, and analytics
- Alerts are prioritized by severity (High, Medium, Low) and mapped to the security framework (e.g. NIST 800-53)



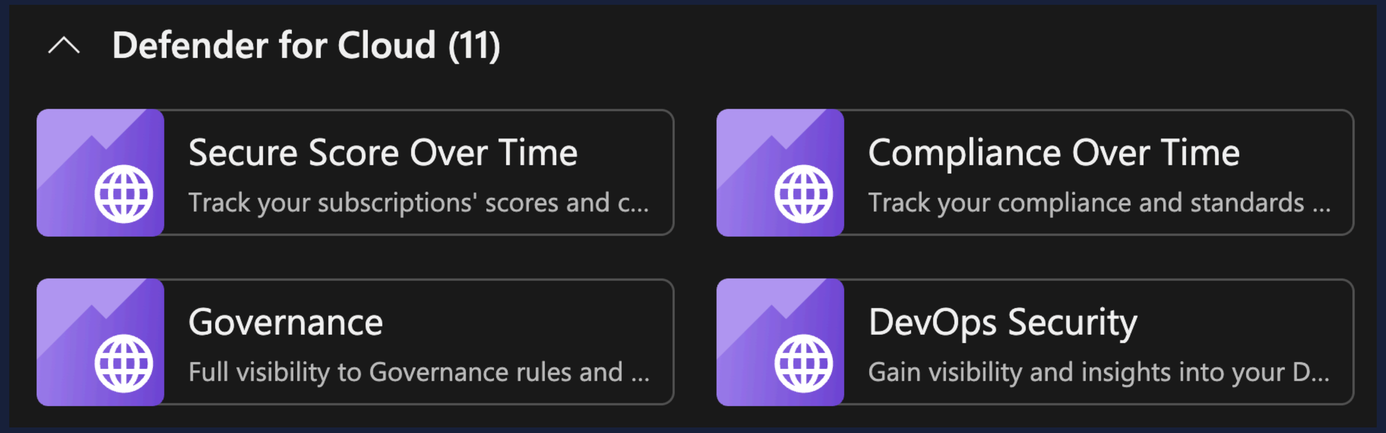
Microsoft Defender for Cloud

@chadmcrowell.com
/in/chadmcrowell
kubeskills.com

CYBR

Export Alert Data to Log Analytics

- KQL queries in Log Analytics
- Creating custom alert rules
- Integration with Microsoft Sentinel
- Build visualizations in Azure Monitor workbooks



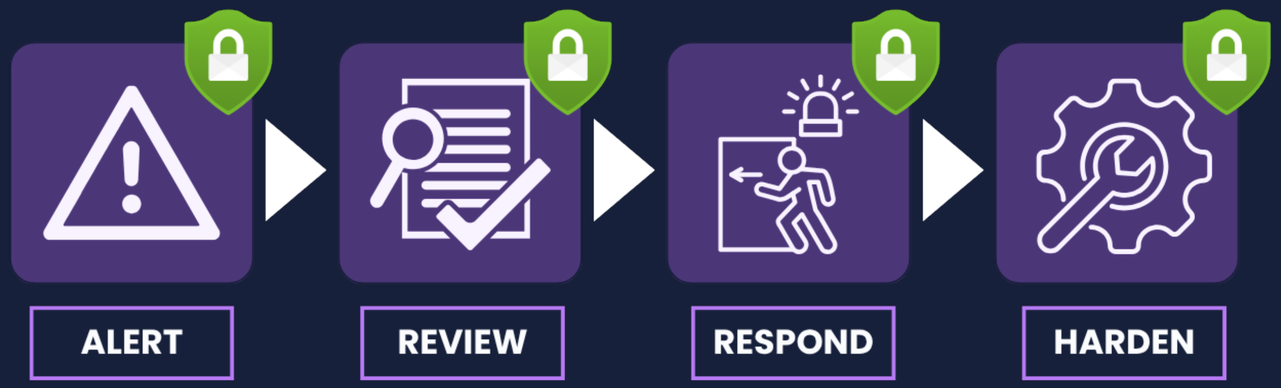
@chadmcrowell.com
/in/chadmcrowell
kubeskills.com

CYBR

Microsoft Defender for Cloud

Real-World Example

- Alert: Suspicious sign-in from a new location.
- Analyst reviews the alert details and impacted assets.
- Uses Defender for Cloud recommendations to block access and harden identity policies.
- Triggers a Logic App to notify the incident response team and isolate the resource if needed.



@chadmcrowell.com
/in/chadmcrowell
kubeskills.com

CYBR

Microsoft Defender for Cloud

Sentinel

- Defender for Cloud alerts can be exported and correlated in Microsoft Sentinel (SIEM/SOAR).
- Enables advanced incident investigation, hunting, and automated response across your entire organization.
- Use Sentinel for a unified view across all security data sources.

@chadmcrowell.com
/in/chadmcrowell
kubeskills.com

CYBR

THANK YOU!